Abraham Schultz HW 1

1.

a)

L	A	R	G	E
S	T	B	C	D
F	H	I/J	K	M
N	O	P	Q	U
V	W	X	Y	Z

b)

O	C	U	R	E
N	A	B	D	F
G	H	I/J	K	L
M	P	Q	S	T
V	W	X	Y	Z

2.) a)

Plain Text as pairs

M	S	S	E	O	O	E	C	J	B	N	E	T	O	I	B	T	N	E
U	T	E	Y	U	V	R	A	O	A	W	S	C	M	N	A	O	C	X

CIPHER TEXT is:

U	T	D	G	P	N	L	T	T	E	O	L	B	U	F	E	H	Q	R
Z	B	L	Z	N	W	G	G	U	R	V	D	D	H	P	R	W	S	Z

Final Encrypted message

UZTBDLGZPNNWLGTGTUERQVLDBDUHFPERHWQSRZ

b) Plaintext same as 2.a, cipher using 1.a matrix

U	T	D	G	P	N	L	T	T	E	O	L	B	U	F	E	H	Q	R
Z	B	L	Z	N	W	G	G	U	R	V	D	D	H	P	R	W	S	Z

UZTBDLGZPNNWLGTGTUERQVLDBDUHFPERHWQSRZ

Abraham Schultz HW1

2.c)

The Results are the same,

This is a Result of the cyclic Rotation of rows and columns. They lead to equivlant substitutions, by Rotating by one step and the rows by Three Steps.

3.a

$$C = (P \oplus k_0) \boxplus k_1$$

C = cipher text
P = plain text
K = secret key
K_0 = leftmost 64 bits of K
K_1 = rightmost 64 bits of K
$\boxplus$ = addition mod 2^{64}

On The Reciever side
let The additive inverse of the key $= (-k_1)$
That is $(c \boxplus -k_1)$
Thus $\boxed{P = (c \boxplus -k_1) \oplus k_0}$

Abraham Schultz HW 1

3.b) $C = (P \oplus K_0) K_1$ $\quad C' = (P' \oplus K_0) \boxplus K_1$

$K_1 = C \boxminus (P \oplus K_0)$ $\quad K_1 = C' \boxminus (P' \oplus K_0)$

$C \boxminus (P \oplus K_1) = C' \boxminus (P' \oplus K_0)$

$C \boxminus C' = (P \oplus K_1) \boxminus (P' \oplus K_0)$

It is not possible to move beyond this point as XOR is NOT distributive binary function.

4) The Feistel cipher proposed goes from $K_1 \ldots K_8 \ldots K_1$

Thus it is actually two 8 Round Feistel ciphers run in reverse order, in a symetric fashion.

This means if I feed C back in to the oracle M will be Retrieved

5.a) Bob knows the First 80 bits of the string (V||C) is V, and thus the rest is C. He has K so he simply has to do the following.

$C \oplus RC4(V||K) = M$

Abraham Schultz HW

5.6)

Because we know (C||V) bit strings. we need only observe the keystream and look for the same V values.
if they are the same, then the same keystream was used.

$$C_1 = RC4(V_1 || k) \oplus m_1$$

$$C_2 = RC4(V_2 || k) \oplus m_2$$

if $V_1 = V_2$ then the same keystream was used.

6.

NO THIS is NOT possible FOR encryption Because each encryption step Relies on the output from the previous step

Decrypting CBC in parallel is possible.

each ciphertext block does not rely on the preceding.
SO if we know all of them we can decrypt them in parallel